

LA LOPD EN EL DÍA A DÍA

¿Quién puede solicitar un derecho ARCO?

Los derechos de acceso, rectificación, cancelación y oposición son personalísimos, y **deben ser ejecutados por el propio afectado**.

Tales derechos se ejercitarán:

- a) **Por el propio afectado**, acreditando su identidad (fotocopia del DNI ó similar).
- b) **Por su representante legal** (siempre acreditado), cuando el afectado se encuentre en situación de discapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos.
- c) **Por un representante voluntario**, expresamente designado para el ejercicio del derecho. En este caso, deberá constar claramente acreditada la identidad del representado, mediante DNI o documento equivalente y la representación conferida por aquél.

Los derechos **serán denegados** cuando la solicitud sea formulada por una **persona distinta del afectado** y no se acredita que actúa en representación de aquél.

Contenido

¿Quién puede solicitar un derecho ARCO?	1
Cartel de videovigilancia no válido	2
Instalación de Call Center en otro país	3
El Tribunal de Justicia de la Unión Europea respalda la tesis...	4
¿Cómo gestiono las altas y bajas de los usuarios en los...	5



IMPORTANTE

Se deben atender los derechos en tiempo y forma, en especial de derecho de cancelación, ya que muchas sanciones de la AEPD se derivan de su omisión.

SANCIONES DE LA AEPD

Cartel de videovigilancia no válido

En el procedimiento sancionador [PS/00328](#) de la AEPD podemos ver la sanción que puede sufrir una empresa si el **cartel informativo de zona videovigilada no cumple con los requisitos** formales establecidos.

Según los hechos, **la Policía Municipal de Madrid denuncia la instalación de cámaras de videovigilancia** en el establecimiento ATOLÓN, titularidad de INVERSIONES ALABARDERO SL, sin cumplir los requisitos exigidos en la LOPD.

Los responsables del local presentaron documentación en la que se hace constar que la **instalación de las cámaras de seguridad ha sido efectuada por la entidad "Securitas Direct"**, así como un CD con fotografías de los carteles instalados en el establecimiento, y en las mismas se puede apreciar que el **cartel instalado recoge: "Securitas Direct. Instalación Protegida. Camaras de videovigilancia 24 horas"** y un número de teléfono.

Sin embargo, según la AEPD, dicho cartel no es conforme a la normativa en materia de protección de datos, porque omite un dato fundamental en la medida en que **no recoge la identidad del responsable del fichero ante el que ejercitar los derechos de acceso, rectificación, cancelación, y oposición** reconocidos en los arts. 15 y siguientes de la LOPD, **así como la referencia a la "Ley Orgánica 15/1999, de Protección de Datos"**.

Resultado: Sanción de 2.000€ por vulneración del artículo 5.1 de la LOPD, relativo al derecho de información.

Es conveniente utilizar el cartel homologado por la Agencia Española de Protección de Datos



IMPORTANTE

El cartel informativo debe incluir la identidad del responsable del fichero y el domicilio ante el cual pueden ejercerse los derechos de acceso y cancelación de las imágenes.

LA AEPD ACLARA

Instalación de Call Center en otro país

El informe [0427/2010](#) de la AEPD resuelve la consulta planteada sobre si resulta exigible lo establecido en la LOPD, en el supuesto planteado en la misma en que la consultante tiene la **intención de instalar en Colombia un servicio de atención de llamadas (call center)** para la atención de los pedidos y reclamaciones de sus clientes, teniendo en cuenta que la empresa **únicamente trata, por regla general, los datos referentes al número de teléfono, fijo o móvil, y domicilio de los citados clientes, con ocasión de la realización de los pedidos que efectúan.** En la consulta se afirma que dichas normas no serían de aplicación al caso, dado que no se estaría procediendo al tratamiento de datos de carácter personal de los clientes.

De dicho informe jurídico se extrae lo siguiente:

- a) El tratamiento de los datos referidos al número telefónico desde el que se realiza un pedido y al domicilio completo en que el mismo ha de entregarse **son datos de carácter personal, sujeto su tratamiento en consecuencia a lo establecido en la Ley Orgánica 15/1999.**
- b) La contratación de un servicio de "call center" en Colombia **implicará una transferencia internacional de datos con destino a un Estado que no ofrece un nivel adecuado de protección**, y para la que será necesario recabar la **autorización del Director** de la Agencia Española de Protección de Datos"

**IMPORTANTE**

Cuando se subcontratan servicios que impliquen el acceso a datos personales con otros países, hemos de tener presente el correcto cumplimiento de la LOPD.

ACTUALIDAD LOPD

El Tribunal de Justicia de la Unión Europea respalda la tesis de la AEPD en relación con los buscadores y el derecho al olvido



Fuente: www.agpd.es



Nota informativa

El Tribunal de Justicia de la Unión Europea respalda las tesis de la AEPD en relación con los buscadores y el derecho al olvido en internet

(Madrid, 13 de mayo de 2014) El Tribunal de Justicia de la Unión Europea (TJUE) ha hecho pública hoy una sentencia de gran trascendencia que resuelve la cuestión prejudicial planteada en marzo de 2012 por la Audiencia Nacional sobre la interpretación de la normativa europea de Protección de Datos (Directiva 95/46/CE) en relación con la actividad de los motores de búsqueda de Internet. La decisión afecta a más de 220 recursos interpuestos por Google contra resoluciones de la Agencia Española de Protección de Datos, actualmente pendientes ante la Audiencia Nacional.

El pronunciamiento del Alto Tribunal, que tiene la última palabra en lo concerniente a la interpretación del derecho de la Unión Europea, **clarifica definitivamente el régimen de responsabilidades** de los buscadores de internet en relación con la protección de los datos personales y **pone término a la situación de desprotección de los afectados generada por la negativa de la compañía Google** a someterse a la normativa española y europea reguladora de la materia.

En la sentencia de hoy el TJUE establece que:

- La actividad de los motores de búsqueda como Google **constituye un tratamiento** de datos de carácter personal, **del que es responsable el propio motor**, dado que éste determina los fines y los medios de esta actividad.
- Ese tratamiento está **sometido a las normas de protección de datos de la Unión Europea**, dado que Google ha creado en un Estado miembro un establecimiento para la promoción y venta de espacios publicitarios y cuya

Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/may_14/NP_STJUE_derecho_olvido.pdf

EL PROFESIONAL RESPONDE

¿Cómo gestiono las altas y bajas de los usuarios en los equipos informáticos para tenerlo todo controlado?

Los procedimientos de control de acceso deben tener en cuenta el **ciclo de vida del usuario**, desde su alta en el sistema, hasta la baja en el mismo.

Para ello, se debe redactar un procedimiento o política de registro de altas y bajas de usuarios, cobrando mayor importancia su estricto cumplimiento, cuantos más usuarios accedan al sistema.

La política debe cumplir, entre otros los siguientes extremos:

- Asignar un **identificador único** por usuario, no compartiendo dicho identificador diferentes usuarios.
- En caso de **baja definitiva** de un usuario, eliminar inmediatamente sus derechos de acceso.
- En caso de **baja temporal**, bloquear su identificador.
- **Revisar periódicamente** la lista de usuarios con la de personal, eliminando usuarios redundantes y los que no están en la lista, así como revisar los recursos a los que tienen acceso.
- **Cotejar la lista de usuarios** anterior con la lista de usuarios y accesos permitidos del Documento de Seguridad.

**IMPORTANTE**

La lista de usuarios con acceso a recursos debe coincidir con la lista de usuarios y accesos permitidos del Documento de Seguridad.